CYBER SECURITY NEWS
Vol. 6 | Issue 2
February 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Happy February! We hope this year is off to a good start for you and your family!

A bit of good news for us, our new cyber security awareness training system is now live! This system is more modern and will allow us to provide updated training material. It also uses our DPS network credentials so those stubborn password resets to get into the training system are a thing of the past!

Thank you to all of you who were first to use this system as your training came due in January. Your feedback was invaluable, and we appreciate your patience as we ride the learning curve along with you.

As a reminder, cyber security awareness training is an annual requirement. When your training is due, you'll be hearing from us; you'll then have 30 days to complete the training. You don't have to do it all in one sitting because it'll save your progress along the way.

A few things to know before launching your training:

- Use FireFox or Edge; Internet Explorer has shown to be problematic, specifically with the CJIS Supplement module.
- This training is not part of the Acadis training system so please use the above URLs to access it. The cyber training URL will also be sent to you when you're notified your training is due.
- These training modules are set up to be completed in sequential order. That way, the "Conclusion" module is done last and sends you an email letting you know you're done and can download your certificate once you've completed all modules.
- If you run into any issues or have any questions, contact us.

Thank you, ahead of time, for your cooperation and attention to this training! We think you'll find it beneficial when navigating technology at home as well. Whether it be with personal email, laptops and smart devices using Wi-Fi, or helping friends and family recognize scams, you'll be better equipped to recognize and avoid cyber crimes. We appreciate your willingness to be cyber vigilant!

Cyber Risk Management

Springtime is just around the corner, and with it typically comes some spring cleaning. Many of us will be cleaning our houses and our garages, maybe even our cars. Our work areas and offices should be on that list as well.

Actually, keeping a clean desk year-round is important. We all need to make sure we don't leave sensitive data lying around for wandering eyes to see. (And, hopefully, you read all about "media marking" in last month's newsletter and clearly marked all that media and data so you know what needs to be locked away!)

Having a desk clear of documents and notebooks, sticky notes, business cards and removable media like USB drives is considered a cyber security best practice.

Now, this does not mean we expect perfectly tidy work areas, fully pristine and well-kept for inspection. No white glove tests for dust bunnies, I promise. But, please be aware of what data is visible or could be easily stolen, and make sure it is kept in a locked drawer or filing cabinet.

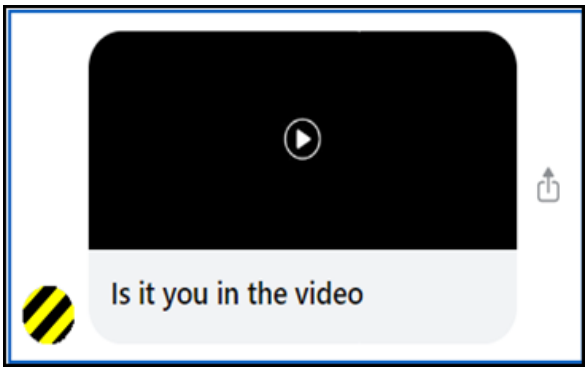
A few tips to help keep a clean desk:

- Don't write passwords or account numbers on sticky notes left on your desk.
- At the end of every workday, clear your desk of documents and papers with DPS information on them.
- Lock away any papers or removable media containing sensitive/confidential data; if these items are no longer needed or necessary, dispose of them properly.
- Lock your computer and stow sensitive documents when you leave your desk, even if you intend to step away for just a few minutes. Take your mobile phone with you.
- Put away all items, including nonessential items and documents, whenever an extended absence is anticipated.
- Keep access cards and keys to the facility on your person at all times.

Following these clean desk practices will help us reduce the risk of information theft, fraud, and security breaches caused by sensitive information being left unattended and visible in plain view.

No, You're Not in That Video

As the pandemic continues, many of us are still keeping in touch with family and friends via Zoom and FaceTime and social media. We are sending one another texts and videos of our families and kids and pets and moments we want others to see so we feel together, even when we aren't.



Scammers know we are all emailing and texting and sharing these photos and videos of one another, and that we generally enjoy seeing these captured memories.

One way they take advantage of this is through apps like Facebook Messenger. If you receive a video with a message similar to "is it you in the video??", don't fall for it. No, that's not you in that video. It's just a way to pique your curiosity and get you to click and then lead you to a fake Facebook login page asking for your username and password. Once you provide those credentials, your account is breached and then used to scam your friends and family. You'll notice that many times, these videos come from a trusted friend...who just happened to fall for the same trick and had their account compromised. Messaging you from a friend's account as opposed to a complete stranger's account is by design.

Paul Ducklin at Sophos's Naked Security blog notes that these messages are much more effective when they come from a trusted account. "From someone you didn't know, a question like that would fall somewhere between bizarre and creepy, but from a friend, who wouldn't want to take a look?" Ducklin says. "There is no video, of course – the black image links to a URL shortening service, which in turn redirects to a URL that pops up what looks like a Facebook login page." Fight the urge to check yourself out!

Other ways to stay safe on Facebook and other social media accounts:

- **Use two-factor authentication (2FA) on any account you can.** Adding a second factor of authentication (like receiving a text with a code after entering your password) means that the crooks can't phish your password alone and then access your account. 2FA is a minor inconvenience to you, but a major roadblock for cybercrimimals.

- **If you think your friend's account has been hacked, contact them via some other method.** Don't reply via the very same account that you don't trust – if it is a scam, you are just tipping off the crooks, who will lie to you and tell you everything is fine.

- **If a friend lets you know your account was hacked, don't delay.** Get into your account as soon as you can (without clicking on any links that anyone just sent you!), assuming you can still access it, and change your password right away so the old password is useless to the criminals.

- **Use a password manager.** Password managers help in many ways: you automatically get a different password for every site; you get passwords that are random and can't be guessed; it's faster to change your password if you do get hacked; and it's much harder to get phished because your password manager won't put the right password into the wrong site.

In the News

Apple says iOS 14.4 fixes three security bugs 'actively exploited' by hackers

(Zack Whittaker | January 26, 2021)

Apple has released iOS 14.4 with security fixes for three vulnerabilities, said to be under active attack by hackers.

The technology giant said in its security update pages for iOS and iPadOS 14.4 that the three bugs affecting iPhones and iPads "may have been actively exploited." Details of the vulnerabilities are scarce, and an Apple spokesperson declined to comment beyond what's in the advisory.

It's not known who is actively exploiting the vulnerabilities, or who might have fallen victim. Apple did not say if the attack was targeted against a small subset of users or if it was a wider attack. Apple granted anonymity to the individual who submitted the bug, the advisory said.

Two of the bugs were found in WebKit, the browser engine that powers the Safari browser, and the Kernel, the core of the operating system. Some successful exploits use sets of vulnerabilities chained together, rather than a single flaw. It's not uncommon for attackers to first target vulnerabilities in a device's browsers as a way to get access to the underlying operating system.

Apple said additional details would be available soon, but did not say when.

It's a rare admission by Apple, which prides itself on its security image, that its customers might be under active attack by hackers.

In the absence of details, iPhone and iPad users should update to iOS 14.4 as soon as possible.

Full Story: https://techcrunch.com/2021/01/26/apple-says-ios-14-4-fixes-three-security-bugs-under-active-attack/

A Few More Cyber News Stories:

ADT Security Camera Flaw Open Homes, Stores to Eavesdropping
https://threatpost.com/adt-security-camera-flaw-opened-homes-stores-to-eavesdropping/163378/

US, European police say they've disrupted the notorious Emotet botnet
https://www.cyberscoop.com/emotet-europol-us-ukraine-takedown-botnet/?category_news=technology

Attackers Leave Stolen Credentials Searchable on Google
https://www.darkreading.com/endpoint/attackers-leave-stolen-credentials-searchable-on-google/d/d-id/1339948

CYBER CHALLENGE

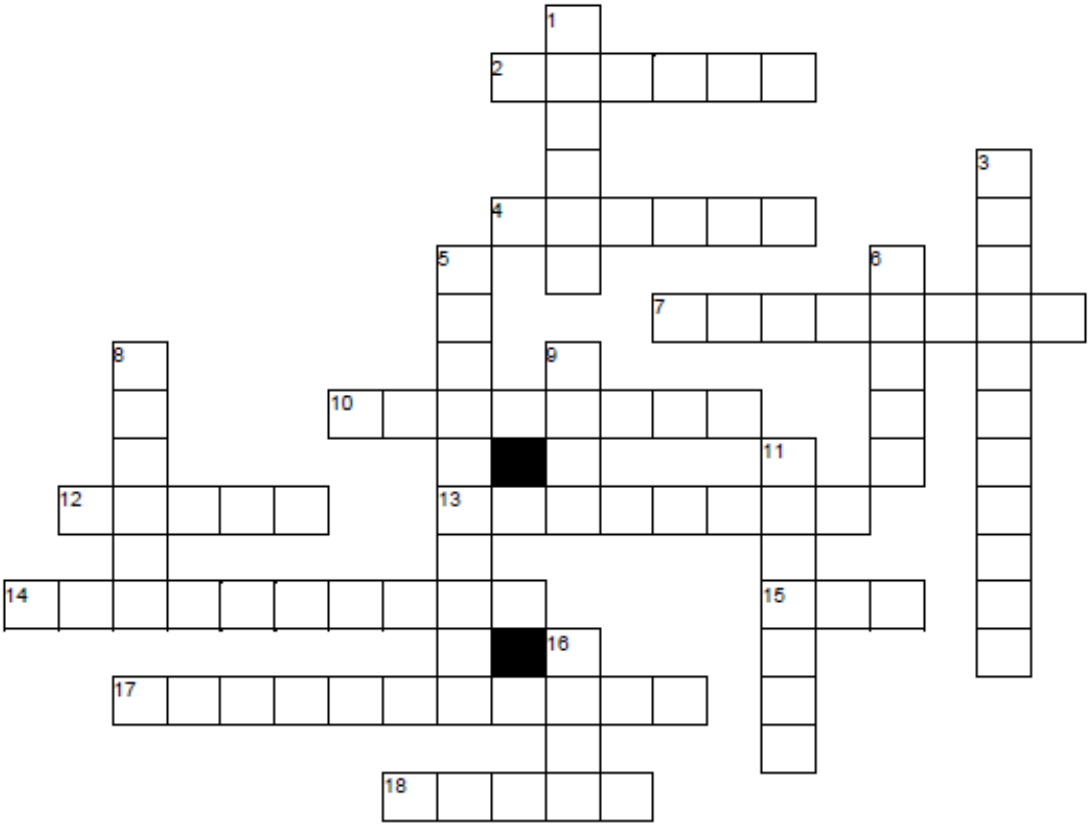
Cyber Crossword Puzzle

This Month's Challenge

For this month's challenge, let's have some fun with the return of a crossword puzzle.

This puzzle's theme is "Remote Office" as many of us continue to work from home and other spots away from our typical DPS offices. Just as before, this was done by a 3rd-party so there are a few answers that you may give the side-eye, but overall, this has some good info. If you get stuck on one of these, ask me for a hint.

Good luck!



Across

2. configure this device for remote office security
4. what to do when something's wrong
7. these messages will always phind you, even when working at home
10. try to separate business and _____ while working remotely
12. the secure place to store files
13. unique for each account
14. a way to protect files when sharing
15. use one of these to connect safely
17. for when we can't see each other in person
18. change your router's _____ password from its default

Down

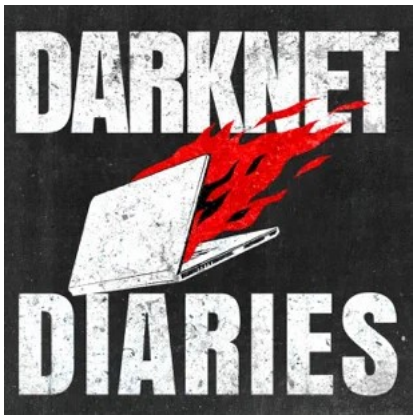
1. your home office should be _____ when you're not there
3. secure _____ are essential to protect data
5. protect this with a PIN or password
6. data or devices in public are vulnerable to this
8. be aware of security when working in _____
9. being careless can lead to _____
11. something you'll want when working on confidential info
16. connect to this with care

</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to take a guess with the last cyber challenge! We fully appreciate you taking a few minutes out of your day to engage with us! Please keep doing so; and get others to join you!

A big THANK YOU to all who submitted an answer!

If you're like me and enjoy a good podcast, I thought I'd share a few cyber-related podcasts that I've found and plan to play in the background throughout my work day and listen to during my commute. Granted, I haven't listened to every episode to each of these so if they get weird or have some colorful language, I apologize in advance! You can find these anywhere you listen to your other podcasts. If you have any cyber or technology podcast favorites, please share them with me. I'll even take suggestions for other genres if it's a can't-miss!



Oh! And we are hiring! We are looking for some summer interns so please take a look at this listing and share it with anybody you feel is qualified and encourage them to apply. Thanks!
DPS - LS - High School Cyber Security Intern (00013331)

Thanks for swinging by, and as always, thank you for your cyber vigilance!

- Eric Posadas